

**IN THE CLAIMS:**

- 1 1. (Currently Amended) A method for certificate generation that enables efficient  
2 revocation of said certificate, comprising:  
3       at a first node:  
4             receiving a request to issue a certificate on behalf of a principal; and  
5             forwarding said request to a second node, wherein said request includes a  
6 first identifier that identifies the first node; and  
7       at the second node:  
8             in response to receipt of the request, generating a certificate that includes said  
9 first identifier.
- 1 2. (Original) The method of claim 1 wherein said request further includes a second  
2 identifier that identifies a principal.
- 1 3. (Original) The method of claim 2 wherein said certificate further includes a public key  
2 associated with said principal, and said second identifier.
- 1 4. (Previously Presented) The method of claim 1 further including authenticating said  
2 certificate by said second node.
- 1 5. (Previously Presented) The method of claim 4 wherein authenticating said certificate  
2 comprises generating a certificate digitally signed by said second node.
- 1 6. (Previously Presented) The method of claim 5 wherein generating said certificate signed  
2 by said second node comprises generating a certificate digitally signed by said second node  
3 using a private key of a public private key pair associated with said second node.
- 1 7. (Original) The method of claim 1 wherein said certificate further includes a time stamp  
2 that identifies a time associated with the request.

1 8. (Previously Presented) The method of claim 1 further including authenticating said  
2 request by said first node.

1 9. (Previously Presented) The method of claim 8 wherein authenticating said request by said  
2 first node comprises digitally signing said request.

1 10. (Previously Presented) The method of claim 9 wherein digitally signing said request  
2 comprises the step of digitally signing said request using a private key of a public/private  
3 key pair associated with said first node.

1 11. (Original) The method of claim 1 wherein said certificate further includes a time stamp  
2 that is associated with a time and date when said request was received by said second node.

1 12-16. (Withdrawn)

1 17. (Currently Amended) A certification authority comprising:

2 a memory containing a computer program for generating a certificate that enables  
3 efficient revocation of said certificate; and

4 a processor operative to execute said computer program, said computer program  
5 containing program code for:

6 receiving a request from a registration authority to issue a certificate on  
7 behalf of a principal; and

8 in response to receipt of said request, generating said certificate that includes  
9 at least a registration authority identifier associated with said registration authority.

1 18. (Original) The certification authority of claim 17 wherein said request to issue said  
2 certificate is an authenticated request and said computer program further includes program  
3 code for verifying said authenticated request.

1 19. (Previously Presented) The certification authority of claim 17 wherein said certificate  
2 generated by said computer program further includes a principal identifier associated with  
3 said principal and a key associated with said principal.

1 20. (Original) The certification authority of claim 17 wherein said computer program  
2 further includes program code for storing within said certificate a time stamp associated with  
3 a time when said certification authority received said request from said registration  
4 authority.

1 21-27. (Withdrawn)

1 28. (Currently Amended) A computer program product including a computer readable  
2 medium, said computer readable medium having a computer program stored thereon for  
3 generating a certificate that enables efficient revocation of said certificate, said computer  
4 program being executable by a processor and comprising:

5 program code for receiving a request from a registration authority to issue a  
6 certificate on behalf of a principal; and

7 program code operative in response to recognition of said request, for generating by  
8 a certification authority a certificate authenticated by said certification authority wherein  
9 said certificate includes at least a principal identifier associated with said principal, a key  
10 associated with said principal for use in authenticating messages generated by said principal,  
11 and a registration identifier associated with said registration authority.

1 29. (Original) The computer program product of claim 28 wherein said program code for  
2 generating said certificate is further operative to include within said certificate a time stamp  
3 associated with a time or receipt by said certification authority of said request from said  
4 registration authority of said request to issue said certificate.

1 30. (Currently Amended) A computer data signal, said computer data signal including a  
2 computer program for use in generating a certificate that enables efficient revocation of said  
3 certificate, said computer program comprising:

4 program code for receiving a request from a registration authority to issue a  
5 certificate on behalf of a principal; and

6           program code operative in response to recognition of said request, for generating by  
7 a certification authority a certificate authenticated by said certification authority wherein  
8 said certificate includes at least a principal identifier associated with said principal, a key  
9 associated with said principal for use in authenticating messages generated by said principal,  
10 and a registration identifier associated with said registration authority.

1   31. (Original) The computer data signal of claim 30 wherein said program code for  
2 generating said certificate is operative to include within said certificate a time stamp  
3 associated with a time of receipt by said certification authority from said registration  
4 authority of said request to issue said certificate.

1   32. (Original) The computer data signal of claim 30 wherein said computer program further  
2 includes program code for publishing said certificate.

1   33. (Previously Presented) The computer data signal of claim 32 wherein said program code  
2 for publishing said certificate includes program code for forwarding said certificate to a  
3 directory server.

1   34. (Currently Amended) An apparatus for generating a certificate in a computer network,  
2 wherein said generating of said certificate enables efficient revocation of said certificate, the  
3 apparatus comprising:

4           means operative in response to receipt of a request from a first node coupled to said  
5 computer network at a second node coupled to said computer network for generating at said  
6 second node a certificate on behalf of a principal that includes a first node identifier  
7 associated with said first node.

1   35. (Currently Amended) The apparatus of claim 34 wherein said request was initiated by-a  
2 said principal and said request includes a principal identifier associated with said principal  
3 and said certificate further includes said principal identifier and a public key associated with  
4 said principal.

1 36. (Original) The apparatus of claim 34 wherein said certificate is authenticated by said  
2 second node.

1 37. (Previously Presented) The apparatus of claim 34 further including means for  
2 comparing said first node identifier to a node identifier associated with an untrustworthy  
3 node on said network that is included within a certificate revocation list and providing an  
4 indication that said certificate is untrustworthy in the event said first node identifier matches  
5 said untrustworthy node identifier.